

EXHIBIT 1

AB:MAA/NCG

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1)
THE PREMISES KNOWN AND
DESCRIBED AS 799 PINE STREET,
APT. 1, BROOKLYN NEW YORK
INCLUDING ANY CLOSED AND
LOCKED CABINETS AND CONTAINERS
FOUND THEREIN; AND (2) THE PERSON
OF SHAKEEM RANKIN (DATE OF
BIRTH: AUGUST 10, 1994) AND THE
AREA WITHIN HIS IMMEDIATE REACH,
INCLUDING ANY PERSONAL EFFECTS
LOCATED THEREIN

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH
WARRANT

Case No. 22-MJ-298

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, ANGELA TASSONE, being first duly sworn, hereby depose and state as
follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"),
and have been for almost eight years. I am currently assigned to the Child Exploitation and
Human Trafficking Task Force, where I investigate violations of criminal law relating to the
sexual exploitation of children. In the course of these investigations, I have reviewed thousands
of photographs depicting children being sexually exploited by adults and have executed search
warrants of premises and electronic devices. Through my experience in these investigations, I
have become familiar with methods of determining whether a child is a minor.

2. I submit this affidavit, pursuant to Federal Rule of Criminal Procedure 41, in support of an application for a warrant and order authorizing the search of:

- a. the premises known and described as 799 Pine Street, Apt. 1, Brooklyn New York (the “PREMISES”), including any closed and locked cabinets and containers found therein. The PREMISES is further described below and in Attachment A.
- b. the person of SHAKEEM RANKIN (date of birth August 10, 1994) and the area within his immediate reach, including any personal effects located therein.

RANKIN is further described below and in Attachment A.

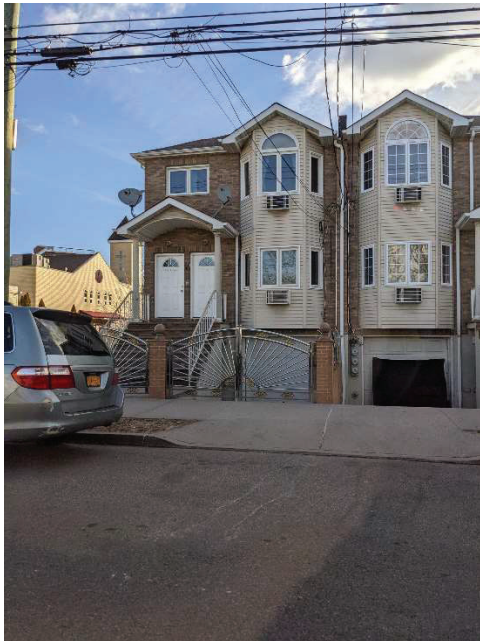
3. Collectively, I refer to RANKIN and the PREMISES as the “SUBJECT PREMISES.” Based on the facts set forth in this affidavit, there is probable cause to believe that a search of the SUBJECT PREMISES will yield evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A (receipt of child pornography, possession of and access with intent to view child pornography), 2252A(a)(2)(A) and (b)(1) receipt and distribution of child pornography, and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography (the “SUBJECT OFFENSES”) committed by SHAKEEM RANKIN and others.

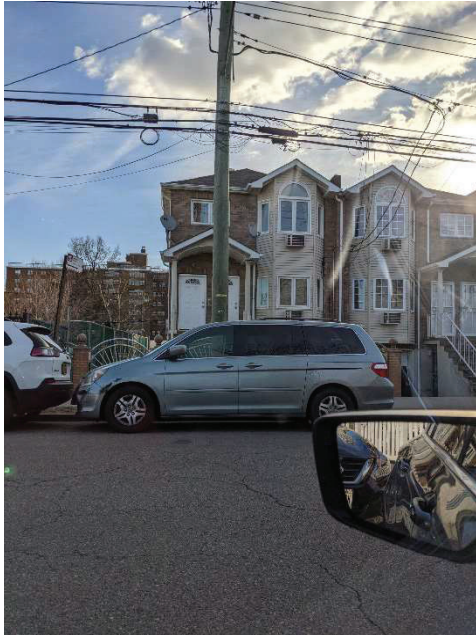
4. This affidavit is based on my training and experience, my personal knowledge of the investigation, my review of relevant records and reports and information obtained from other law enforcement agents, and my training and experience concerning the use of criminal activity and the forensic analysis of electronically stored information (“ESI”). This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the contents of documents and

the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

RANKIN AND THE PREMISES

5. The PREMISES is a multi-level residential dwelling located at 799 Pine Street, Apt. 1, Brooklyn New York. The building containing the PREMISES is brick, with part of it painted in a tan color and with white trim. The building containing the PREMISES contains two apartments. There are two white front doors at the front of the building, accessed by going up a flight of outside steps, with the door on the right (while facing the apartment) leading to Apartment 1 and the door on the left leading to Apartment 2. The following photographs depict the building containing the PREMISES:





6. RANKIN was born on August 10, 1994. He is a 28-year-old male who stands approximately 5 feet 10 inches tall. He has a dark-skinned complexion, black hair, and brown eyes. As described further herein, there is probable cause to believe that RANKIN will be present at the PREMISES at the time the search warrant is executed and may have instrumentalities used to commit the SUBJECT OFFENSES—particularly, cellular telephones—on his person at that time. A photograph of RANKIN is in Attachment A.

7. Based on open-source information, RANKIN currently resides at the PREMISES. At least one other adult male and one adult woman, all seemingly relatives of RANKIN's, seemingly also live at the PREMISES. Upon information and belief, RANKIN's relatives also live in Apartment 2.

8. This application seeks authorization to search the entirety of the PREMISES, as well as all attachments, attics, basements, garages (including the detached garage), carports, vehicles, outbuildings, storage units, appurtenances thereto, and all other areas

within the curtilage, and all closed and locked containers and electronic devices located therein; however, this application does not seek authorization to search Apartment 2.

9. This application also seeks authorization to search RANKIN and the area within his immediate reach, including any personal effects located therein.

PROBABLE CAUSE

The SUBJECT OFFENSES

10. Law enforcement officers currently are investigating RANKIN for distribution, receipt, and possession of child pornography.

11. Based on my conversations with other law enforcement officers involved in this investigation, my review of law enforcement reports and records, I have learned the following, in substance and in part:

12. Law enforcement officers have been investigating an individual (“Subject 1”) in St. Louis, Missouri, for production and distribution of child sexual abuse material (“CSAM”). Based on its investigation, law enforcement has determined that Subject 1 produced CSAM with his 9-year-old niece and advertised CSAM on Tumblr and Reddit. Subject 1’s advertisements directed individuals interested in CSAM to communicate with Subject 1 via Kik Messenger (also known as “Kik”), a mobile chat application that allows individuals to, among other things, engage in group conversations and share photographs and videos. Using Kik, Subject 1 negotiated prices to be paid to him for CSAM via “Cash App,” an application that enables users to send and receive money. After Subject 1 received the agreed-upon money, Subject 1 sent buyers links to CSAM images and/or videos using MEGA, an application that enables users to share files.

13. On or about May 4, 2021, law enforcement executed a judicially-authorized search warrant at Subject 1's residence. Pursuant to the search warrant, law enforcement searched Subject 1's cellular phones, on which they found Kik conversations.

14. Based on information recovered from Subject 1's phone, one of the buyers of MEGA links was Kik user "mulaDussa" (the "Subject Kik Account"). The links purchased by the Subject Kik Account contained over 2000 videos and images that law enforcement agents were able to identify as CSAM.

15. According to Kik chat logs, on or about April 9, 2021, Subject 1 sent messages to the Subject Kik Account asking if the Subject Kik Account wanted "cp," which Subject 1 described as "young young young content no preteens younger than preteens." After Subject 1 seemingly provided examples, Subject 1 stated "I got better stuff if u wanna buy." The Subject Kik Account responded "yeah I want all the Cp lol." Subject 1 instructed the Subject Kik Account to "Send \$80 I got u," and a few minutes later, the Subject Kik Account responded "Sent." Subject 1 then sent, among other things, links to MEGA and stated "If u want more let me kno."

16. According to Kik chat logs, on or about April 25, 2021, the Subject Kik Account asked Subject 1 to re-send "that link," explaining "It's not popping up anymore for some reason." Subject 1 responded "Resend fee," to which the Subject Kik Account asked "80?" and Subject 1 replied "Yop" and seemingly provided information for a new Cash App account. The Subject Kik Account requested "Send more Black girls if u got," in response to which Subject 1 subsequently stated "all black cp giant file there u go" and seemingly sent a MEGA link. The Subject Kik Account then asked about "the regular cp from B4," to which Subject 1 seemingly sent a MEGA link.

17. Based on information recovered from Subject 1's phone, Cash App user "Shamula" sent Subject 1 approximately \$80 on or about April 9, 2021 and another approximately \$80 on or about April 25, 2021, *i.e.*, on the dates of the Kik chats described above.

18. Based on subpoena returns from Kik, the email address associated with the Subject Kik Account is blab705@yahoo.com. The Kik subpoena returns also include the IP address used by the Subject Kik Account to access Kik. Based on subpoena returns from Verizon, the physical address associated with the IP address is the PREMISES, without the apartment number specified, in the name of "Jem Rankin," who law enforcement believes to be a relative of RANKIN's.

19. Based on Yahoo returns for the Yahoo blab705@yahoo.com email account, the associated telephone number is 212-518-8371. Based on open sources, the subscriber for that phone number is RANKIN.

20. To date, law enforcement officers have not been able to determine the MEGA accounts associated with the Kik chats between Subject 1 and the Subject Kik Account on April 9, 2021 and April 25, 2021. However, information from MEGA indicates an active account by user blab705@yahoo.com, *i.e.*, the same email address associated with the Subject Kik Account. Information from MEGA also includes the IP address from which user blab705@yahoo.com accessed MEGA, which is the same IP address used by the Subject Kik Account to access Kik. As indicated above, the physical address associated with this IP address is the PREMISES, without the apartment number specified.

21. Based on my training and experience, and the foregoing, I believe that RANKIN is the user of the Subject Kik Account and the blab705@yahoo.com MEGA account.

Moreover, given that the payment dates and amounts made from the “ShaMula” Cash App account correspond with the payment dates and amounts by the Subject Kik Account referenced in the Kik chats with Subject 1, I believe that RANKIN is the user of the “ShaMula” Cash app account.

22. On March 14, 2022, I conducted surveillance outside the PREMISES, and I observed RANKIN exit Apartment 1.

23. Based on my training and experience, I know that individuals who maintain and transmit child pornography often maintain lists of names, email addresses, telephone numbers, and screen names of others with whom they can share child pornography, and frequently do share child pornography with others. I also know that producers and collectors of child pornography typically retain their materials for extended periods of time. In this case, RANKIN twice purchased links containing over 2000 videos and images that law enforcement agents were able to identify as CSAM, and he asked for additional CSAM focused on a particular race and gender, in response to which he received a collection of materials. RANKIN therefore appears to be a collector of CSAM. Producers and collectors of child pornography frequently collect and view sexually explicit materials in a variety of media, such as videos, photographs, magazines, books, drawings, and other visual media that they use for sexual arousal and gratification. These examples of visual media are often stored on electronic devices including, but not limited to, phones, computers, disk drives, modems, thumb drives, digital cameras, and scanners.

24. In addition, based on my training and experience, I know that while individuals might delete chats, photographs and videos from their electronic devices, the metadata on electronic devices retains the chats, photographs and videos significantly longer.

Specifically, I know that chats, photographs and videos from Kik are recoverable for a significant period of time through searching the metadata, including with respect to deleted files. Finally, based on my training and experience, I know that individuals who possess and operate electronic devices often store, maintain, and/or utilize those devices in their place of residence.

25. Based on my training and experience, and the foregoing, I submit there is probable cause to believe that RANKIN has received images and videos of child pornography while physically present at the PREMISES. Moreover, I submit there is probable cause to believe that the SUBJECT PREMISES contain evidence, instrumentalities, contraband, and fruits of the SUBJECT OFFENSES.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

32. In addition to there being probable cause to believe that phones and/or computer devices will be found on the SUBJECT PREMISES that contain evidence of the SUBJECT OFFENSES, there also is probable cause to believe that these devices constitute instrumentalities and/or contraband subject to seizure, in that the devices were used to commit the SUBJECT OFFENSES and contain contraband child pornography.

33. *Biometric Unlocking.* In my training and experience, it is likely that if a subject has any electronic devices on his person or in his belongings, then one or more of those devices uses biometric unlocking features, such as facial recognition unlocking. The warrant I am applying for would permit law enforcement to compel the subject to unlock any electronic devices using the devices' biometric features. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many

electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain cellular phone devices. In order to activate this unlocking mechanism, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.
- d. If a device is equipped with an iris recognition feature, a user may enable the

ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared sensitive camera detects the registered irises. Iris recognition features on other manufacturers’ devices have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. I also know from my training and experience, as well as from information found in publicly available materials, including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked, or (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or

password has not been entered in the last six days. Biometric features from other electronic device brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- g. The passcode or password that would unlock a given device recovered during execution of the requested warrant likely will not be known to law enforcement. Thus, in attempting to unlock any such devices for the purpose of executing the search authorized by the requested warrant, it will likely be necessary to press the finger(s) of the user on the fingerprint reader of any device capable of biometric unlocking. The government may not otherwise be able to access the data contained on the electronic devices for the purpose of executing the search authorized by this warrant.
- h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

34. Due to the foregoing, if any of RANKIN's electronic devices may be unlocked using one of the aforementioned biometric features, then the warrant I am applying for would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of RANKIN against the fingerprint scanner of the device; (2) hold RANKIN in place while holding the device in front of his face to activate the facial recognition feature; and/or (3) hold RANKIN in place while holding the device in front of his face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by

this warrant.

35. Based on the foregoing, I respectfully submit there is probable cause to believe that RANKIN committed the SUBJECT OFFENSES, and that evidence of this criminal activity is likely to be found in the PREMISES and in the closed containers/items stored therein, including any electronic devices found on RANKIN's person while he is physically present in the PREMISES.

A. Execution of Warrant for ESI

36. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," including for "later review." Consistent with Rule 41, this application requests authorization to seize the items listed in Attachment B and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

37. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

38. An item may be seized if law enforcement officers reasonably believe that (a) the item belongs to RANKIN, based on the location of the item, identifying information on the exterior of the device, other information available to the officers, and statements made by residents of the PREMISES at the time of the search, and (b) the item does not otherwise appear to belong to a resident of the PREMISES who is not involved in the commission of the SUBJECT OFFENSES.

B. Review of ESI

39. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

40. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

41. If the government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the government will return these items. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the SUBJECT OFFENSES.

CONCLUSION

42. Based on the foregoing, there is probable cause to believe that a search of the SUBJECT PREMISES described in Attachment A to search for and/or seize the items set forth in Attachment B will uncover evidence, fruits, instrumentalities or contraband of the SUBJECT OFFENSES.

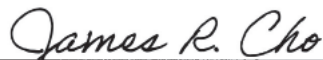
43. I respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this affidavit and the search warrant. These documents discuss an ongoing criminal investigation that is neither public nor known to the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure might seriously jeopardize that investigation, including by giving subjects an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Angela Tassone', written over a horizontal line.

Angela Tassone
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone
on March 15, 2022


HONORABLE JAMES R. CHO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

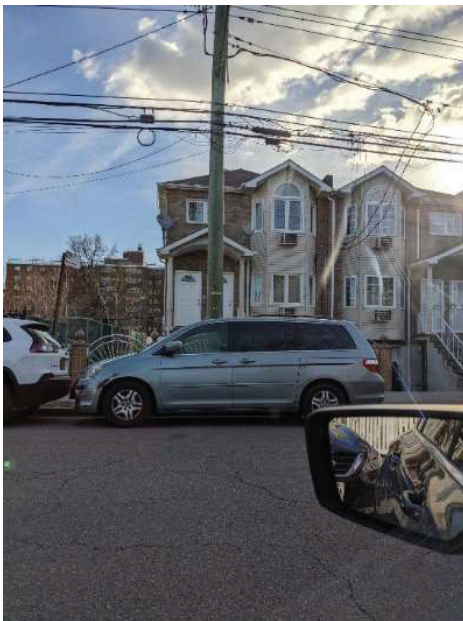
Premises to Be Searched

The person of SHAKEEM RANKIN (date of birth August 10, 1994) and the area within his immediate reach, including any personal effects located therein. RANKIN is a 28-year-old male who stands approximately 5 feet 10 inches tall. He has a dark-skinned complexion, black hair, and brown eyes. He is pictured here:



The premises to be searched includes is a multi-level residential dwelling located at 799 Pine Street, Apt. 1, Brooklyn New York (“the SUBJECT PREMISES”). The building containing the SUBJECT PREMISES is brick, with part of it painted in a tan color and with white trim. The building containing the SUBJECT PREMISES contains two apartments. There are two white front doors at the front of the building, accessed by going up a flight of outside steps, with

the door on the right (while facing the apartment) leading to Apartment 1 and the door on the left leading to Apartment 2. The following photographs depict the building containing the
SUBJECT PREMISES:



ATTACHMENT B

Property to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized include the following evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A (receipt of child pornography, possession of and access with intent to view child pornography), 2252A(a)(2)(A) and (b)(1) receipt and distribution of child pornography, and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography (the “SUBJECT OFFENSES”) committed by SHAKEEM RANKIN and others, described as follows:

1. Computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES. For purposes of this Attachment A, computer devices, storage media, and related electronic equipment includes, but is not limited to, any computer, computer system and high-speed data processing device, including, but not limited to, desktop computers, notebook computers, tablets, and server computers; mobile phones, including, but not limited to, smart phones capable of transmitting electronic messages (such as text messages and email messages); tapes; cassettes; cartridges; streaming tape; commercial software and hardware; network hardware and software; computer disks; disk drives; monitors; computer printers; modems; tape drives; disk application programs; data disks; system disk operating systems; tape systems and hard drive and other computer related operation equipment; routers, modems, and network equipment used to connect to the Internet; cameras; video cameras; scanners; computer photographs; graphic interchange formats and/or photographs; undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG); any electronic data storage devices including, but not limited to, hardware, software, diskettes, magnetic media floppy disks; backup tapes, CD-ROMs, DVDs, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including, but not limited to, data security devices;
2. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
3. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
4. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
5. Correspondence and records pertaining to violation of the SUBJECT OFFENSES including, but not limited to, envelopes, letters, mailings, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction,

receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

6. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;
7. Any child pornography as defined by 18 U.S.C. § 2256(8);
8. Any visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
9. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, electronic mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
10. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
11. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES, including, but not limited to, sales receipts, warranties, bills for Internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs;
12. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence; and
13. Evidence that SHAKEEM RANKIN subscribed to and accessed Kik, and any other evidence relating to Kik that demonstrates user attribution.

An item may be seized if law enforcement officers reasonably believe that (a) the item belongs to SHAKEEM RANKIN, based on the location of the item, identifying information on the exterior of the device, other information available to the officers, and statements made by residents of the PREMISES at the time of the search, and (b) the item does not otherwise appear

to belong to a resident of the PREMISES who is not involved in the commission of the SUBJECT OFFENSES.

B. Search and Seizure of ESI

The items to be seized also include any computer devices and storage media that may contain any electronically stored information (“ESI”) falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the Government in this investigation, and outside technical experts under Government control) are authorized to review the ESI contained therein for information responsive to the warrant.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other ESI within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

D. Biometric Unlocking

If it is determined that one or more of electronic devices covered by this warrant can be enabled or unlocked with “Touch ID” or other biometric unlocking features, law enforcement officers are authorized to (1) press or swipe the fingers (including thumbs) of RANKIN against the fingerprint scanner of the device; (2) hold RANKIN in place while holding the device in front of his face to activate the facial recognition feature; and/or (3) hold RANKIN in place while holding the device in front of his face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.